Note di Matematica
Note Mat. **37** (2017) no. 1, 41–51.
ISSN 1123-2536, e-ISSN 1590-0932
doi:10.1285/i15900932v37n1p41

The State of the Art on the Conjecture of Exceptional APN Functions

Moisés Delgado
University of Puerto Rico, Cayey Campus
Mathematics and Physics Department
Cayey, PR 00736, USA
moises.delgado@upr.edu

Received: 26.1.2016; accepted: 2.2.2017.

Abstract. The well known conjecture about exceptional almost perfect non-linear (exceptional APN) functions, stated by Aubry, McGuire and Rodier, says that the monomials x^{2^k+1} and $x^{2^{2k}-2^k+1}$, the Gold and Kasami-Welch functions respectively, are the only ones in this class. Many results have been obtained in the last years confirming the conjecture. In this article we list all these settled results, all the pending cases, and provide a new family of non exceptional APN functions. Also, we comment the methods used to obtain the resolved cases and propose a provable new one, using the Max Noether's Fundamental theorem, to overcome some pending cases.

Keywords: Almost perfect nonlinear, exceptional almost perfect nonlinear, absolute irreducibility, bezout's theorem, Max Noether's theorem.

MSC 2000 classification: primary 11Txx, secondary 11T71

1 Introduction

The study of APN functions arose approximately 23 year ago when Biham and Shamir [3] introduced differential cryptanalysis as a potential attack for DES-like ciphers. APN functions, as defined and proved by Nyberg [17, 18], have the property of being high resistant against differential attacks when they are used as substitution components of block ciphers.

Definition 1. Let $L = \mathbb{F}_q$, with $q = 2^n$ for some positive integer n. A function $f : L \to L$ is said to be *almost perfect nonlinear* (APN) on L if for all $a, b \in L$, $a \neq 0$, the equation

$$f(x + a) - f(x) = b \tag{1}$$

have at most 2 solutions.

The best known examples of APN functions are the family of Gold functions $f(x) = x^{2^k+1}$, which are APN on any field $\mathbb{F}_{2^n}$ where k, n are relatively prime

integers. Other examples are the family of Welch functions $f(x) = x^{2^r+3}$ which are APN on $\mathbb{F}_{2^n}$, where $n = 2r + 1$.

The APN property is invariant under some transformations of functions. A function $f : L \to L$ is called *affine* if

$$f(x) = a + \sum_{i=0}^{n-1} a_i x^{2^i}, \quad a, a_i \in L$$

Two functions are Carlet, Charpin, Zinoviev equivalent (CCZ-equivalent) if the graph of f, $\{x, f(x)\}$, can be obtained from the graph of g, $\{x, g(x)\}$, by an affine permutation. Two CCZ-equivalent functions preserves the APN property. Mostly, the CCZ-equivalence is very hard to prove (for more details see [5]).

Notice that, as shown in the above examples, the APN property may depends on the extension degree of $\mathbb{F}_2$. For any $t = 2^r + 1$ there exist infinitely many values m such that $(r, m) = 1$. That is, any fixed Gold function which is APN on L is also APN on infinitely many extensions of L. Functions with this property are called **exceptional** APN functions. The situation is different for our second example, a Welch function that is APN over L is not necessarily APN on an extension of L.

Definition 2. Let $L = \mathbb{F}_q$, $q = 2^n$ for some positive integer n. A function $f : L \to L$ is called **exceptional APN** if f is APN on L and also on infinitely many extensions of L.

One way to classify APN functions is to determine which of them has the property of been exceptional. This problem has been studied for monomials functions by Janwa, Wilson, Canteaut, McGuire, Jedlika and Hernando [4, 13, 14, 15, 16] and more recently for polynomials by Aubry, McGuire, Rodier, Caullery, Delgado, Janwa, Ferard and Oyono [1, 6, 7, 8, 21]. Aubry, McGuire and Rodier conjectured the following [1].

CONJECTURE: Up to equivalence, the Gold and Kasami-Welch functions, $f(x) = x^{2^k+1}$ and $f(x) = x^{2^{2k}-2^k+1}$ respectively, are the only exceptional APN functions.

The names Gold and Kasami-Welch are due to the degree of the monomials, the well known families of Gold and Kasami-Welch numbers $2^k + 1$, $2^{2k} - 2^k + 1$, for $k \geq 1$ respectively. This is the sequence number AO64386 in the On-line Encyclopedia of Integer sequences.

The conjecture is settled for monomial functions. Hernando and McGuire [13], based on the work of Janwa and Wilson [15] and a partial result of Jedlicka [16], proved that the Gold and Kasami-Welch functions are the only exceptional

APN monomial functions. For non monomial functions, the conjecture is still open.

The goal of this article is to provide an overview of all the obtained results which contribute to the proof of the mentioned conjecture. The article is organized as follows. In section 2, a very important Rodier's result, which make a link between the exceptional property of a function f and the set of rational points of an affine surface X defined by f, is shown. This result provides a criteria for proving that f can not be exceptional APN. In section 3 and 4, considering the degree of the functions, we list all the resolved and pending cases about this conjecture. In section 5, we make a remark on the results obtained for the Gold degree case, which lead us to obtain a new infinite family of non exceptional APN polynomials. Finally, in section 6, we briefly comment the used methods in each of the obtained results and propose a provable new method to overcame some of the pending cases.

2 Absolute irreducibility and the exceptional property

Let $L = \mathbb{F}_q$, $q = 2^n$ for some positive integer n. Rodier, using algebraic geometry concepts, characterized APN functions and proposed a criteria for these functions to be exceptional APN [19].

Rodier proved that a function $f : L \to L$ is APN if and only if the rational points of the affine surface

$$f(x) + f(y) + f(z) + f(x + y + z) = 0$$

are contained in the surface $(x + y)(x + z)(y + z) = 0$.

Let f be a polynomial function in $L[x, y, z]$, $\deg(f) = d$. Let us define:

$$\phi(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(x + z)(y + z)} \tag{2}$$

Then ϕ is a polynomial over $L[x, y, z]$ of degree $d - 3$. This polynomial defines a surface X in the three dimensional affine space L^3.
It can be shown that if $f(x) = \sum_{j=0}^{d} a_j x_j$, then:

$$\phi(x, y, z) = \sum_{j=3}^{d} a_j \phi_j(x, y, z)$$

where

$$\phi_j(x, y, z) = \frac{x^j + y^j + z^j + (x + y + z)^j}{(x + y)(x + z)(y + z)} \tag{3}$$

is homogeneous of degree $j-3$.

From the above characterization and the results of Lang-Weil and Ghorpade-Lachaud [12], which guarantees enough L-rational points on a surface for n sufficiently large, it can be deduced the next theorem whose proof can be found in [19].

Theorem 2.1. Let $f : L \to L$ a polynomial function of degree d. Suppose that the surface X of affine equation

$$\frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)} = 0$$

is absolutely irreducible (or has an absolutely irreducible component over L) and $d \geq 9$, $d < 0.45q^{1/4} + 0.5$, then f is not an APN function.

This theorem establish the criteria that, if X is absolutely irreducible (or has an absolutely irreducible factor over L) then f is not exceptional APN.

3 Resolved cases

In this section we list all the families of functions for which the statement of the conjecture is proved. From now on, let $L = \mathbb{F}_{2^n}$ for n a positive integer.

Let us divide the cases according to the degree of the families.

3.1 Odd degree case

The conclusions of the next theorems follows by proving that the function is absolutely irreducible or contain an absolutely irreducible factor.

As commented before, the conjecture is proved for monomial functions. Hernando and McGuire completed the proof of the conjecture on the sequence of exceptional numbers [13], which can be stated equivalently as follows.

Theorem 3.1. (Hernando, McGuire [13]) The Gold and Kasami-Welch functions are the only exceptional APN monomial functions.

The next theorems refers to non monomial functions.

Theorem 3.2. (Aubry, McGuire, Rodier [1]) If the degree of the polynomial function f is odd and not a Gold or a Kasami-Welch number, then f is not exceptional APN

Aubry, McGuire and Rodier also found results for Gold degree polynomials.

Theorem 3.3. (Aubry, McGuire, Rodier [1]) Suppose $f(x) = x^{2^k+1} + g(x) \in L[x]$ where $\deg(g) \leq 2^{k-1}+1$. Let $g(x) = \sum_{j=0}^{2^{k-1}+1} a_j x^j$. Suppose that there

exists a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then f is not exceptional APN.

The authors remarked that, in theorem 4, the weaker condition of being both ϕ_{2^k+1} and ϕ_j relatively prime is sufficient.

They also studied the case when $\deg(g) = 2^{k-1} + 2$.

Theorem 3.4. (Aubry, McGuire, Rodier [1]) Suppose $f(x) = x^{2^k+1} + g(x) \in L[x]$ and $\deg(g) = 2^{k-1} + 2$. Let k be odd and relatively prime to n. If $g(x)$ does not have the form $ax^{2^{k-1}+2} + a^2x^3$ then ϕ is absolutely irreducible, while if $g(x)$ does have this form, then either ϕ is absolutely irreducible or ϕ splits into two absolutely irreducible factors that are both defined over L.

In the next two theorems, the authors extended these two previous results.

Theorem 3.5. (Delgado, Janwa [7])For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$, where $\deg(h) \equiv 3 \pmod 4 < 2^k + 1$. Then f is not exceptional APN.

Theorem 3.6. (Delgado, Janwa [7]) For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$ where $d = \deg(h) = 1 \pmod 4 < 2^k + 1$. If ϕ_{2^k+1}, ϕ_d are relatively prime, then f is not exceptional APN.

It is clear that this last theorem applies for the cases when ϕ_d is absolutely irreducible. In [10], Férard provided sufficient conditions for this irreducible fact to happen, when $d = 5 \pmod 8$, with the next theorem.

Theorem 3.7. (Ferard, [10]) Let l be an odd integer, $l \geq 7$, $t = 4l + 1$ and $\phi_t(x, y, 1)$ as in equation (3). We assume that there are no points $(x, y) \in \left(\overline{\mathbb{F}_2}\right)^2$ which satisfy the following system

$$\begin{cases} x \neq 1, y \neq 1, x \neq y \\ x^l = 1, y^l = 1, (x + y + 1)^l = 1 \\ \phi_{13}(x, y) = 0 \end{cases}$$

Then the polynomial ϕ_t is absolutely irreducible.

Using this theorem, Ferard verified, with the aid of SAGE, that ϕ_t is absolutely irreducible for all t, $t = 5 \pmod 8$, $13 < t < 205$.

In the same direction, Delgado et.al proved that the relatively prime condition of theorem 7 is satisfied for all $d = 5 \pmod 8$ [9]. Very recently, theorem 7 was improved with the next one without conditions.

Theorem 3.8. (Delgado, Janwa [8]) For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$ where $\deg(h) = 1 \pmod 4 < 2^k + 1$ ($\deg(h)$ is not a Gold number), then f is not exceptional APN.

The case for Kasami-Welch degree polynomials seems to be the hardest one. Ferard, Oyono and Rodier proved the following two theorems.

Theorem 3.9. (Ferard, Oyono and Rodier [20]) Suppose that $f(x) = x^{2^{2k}-2^k+1} +$

$g(x) \in L[x]$ where $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Suppose moreover that there exist a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then f is not exceptional APN.

They also studied the case when $\deg(g) = 2^{2k-1} - 2^{k-1} + 2$ [21].

Theorem 3.10. (Ferard, Oyono and Rodier [20]) Suppose that $f(x) = x^{2^{2k}-2^k+1} + g(x) \in L[x]$ where $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 2$. Let $k \geq 3$ be odd and relatively prime to n. If $g(x)$ does not have the form $ax^{2^{2k-1}-2^{k-1}+2} + a^2x^3$ then ϕ is absolutely irreducible, while if $g(x)$ does have this form then either ϕ is irreducible or ϕ splits into two absolutely irreducible factors which are both defined over L

3.2 Even degree case

For this case, very few results have been established.

Theorem 3.11. (Aubry, McGuire, Rodier [1]) If the degree of the polynomial function f is $2e$ with e odd, and if f contains a term of odd degree, then f is not APN over $L = \mathbb{F}_{q^n}$ for all n sufficiently large.

For polynomials of degree $4e$, Rodier proved the following:

Theorem 3.12. (Rodier [21]) If the degree of the polynomial function f is even such that $\deg(f) = 4e$ with $e \equiv 3(\mod 4)$ and if the polynomials of the form $(x + y)(y + z)(z + x) + P$ with

$$P(x, y, z) = c_1(x^2 + y^2 + z^2) + c_4(xy + xz + yz) + b_1(x + y + z) + d$$

for $c_1, c_4, b_1, d \in \mathbb{F}_{q^3}$, do not divide ϕ then f is not exceptional APN.

Florian Caullery extended the last result with the next theorem.

Theorem 3.13. (Caullery [6]) Let $f : \mathbb{F}_q \to \mathbb{F}_q$ of degree $4e$ with $e > 3$ such that ϕ_e is absolutely irreducible. Then f is not a exceptional APN function.

4 Pending cases

Given the list of results in section 3 and a subsequent result in section 5, the list of pending cases are:

4.1 Odd degree case

Gold degree functions:

- $f(x) = x^{2^k+1} + h(x) \in L[x]$, where $\deg(h)$ is a Gold number and $(\phi_{2^k+1}, \phi_j) \neq 1$ for all j in $h(x) = \sum a_j x^j$.

- $f(x) = x^{2^k+1} + h(x) \in L[x]$, where $d = \deg(h)$ is an even number, $d \geq 2^{k-1} + 2$.

  The case $d = 2^{k-1} + 2$ is only partially resolved (see theorem 5).

Kasami-Welch degree functions:

- $f(x) = x^{2^{2k}-2^k+1} + h(x) \in L[x]$, where $\deg(h) \geq 2^{2k-1} - 2^{k-1} + 2$.

  The case $\deg(h) = 2^{2k-1} - 2^{k-1} + 2$ is only partially resolved (see theorem 11)

4.2 Even degree case

- $f(x) \in L[x]$ such that $\deg(f) = 2e$, where e is an odd number and f have only even degree terms.
- $f(x) \in L[x]$ such that $\deg(f) = 4e$, such that ϕ_e is not absolutely irreducible.

5 A new family

Stated the theorems 6 and 9, the conjecture is done for Gold degree polynomials of the form $f(x) = x^{2^k+1} + h(x)$, where $d = \deg(h)$ is any odd number (not a Gold number). Then, the remaining case is when d is a Gold number.

For polynomials of the form $f(x) = x^{2^k+1} + h(x)$, where $\deg(h) = 2^{k'} + 1$ and $(k, k') = 1$, $\phi_{2^k+1}, \phi_{2^{k'}+1}$ are relatively prime [7]. Then $\phi(x, y, z)$ is absolutely irreducible by theorem 7.

For non relatively prime numbers k, k', assuming reducibility of ϕ:

$$\phi(x, y, z) = (P_s + P_{s-1} + ... + P_0)(Q_t + Q_{t-1} + ... + Q_0) \tag{4}$$

where P_i, Q_i are zero or forms of degree i.

Equating the homogeneous terms degree by degree, as in the proof of theorem 7 (first case) [7], we have that: $Q_{t-1} = Q_{t-2} = ... = Q_1 = Q_0 = 0$ (Observe in this proof that $t < e$, where $e = 2^k + 1 - d$).

Then, the surface ϕ related to f factors as:

$$\sum_{j=3}^{2^k+1} a_j \phi_j(x, y, z) = (P_s + P_{s-1} + ... + P_0)(Q_t)$$

Therefore Q_t divides each $\phi_j(x, y, z)$. This implies that $\phi(x, y, z)$ would be absolutely irreducible if h contains a non zero term $a_m x^m$ such that ϕ_{2^k+1} and ϕ_m are relatively prime.

Using the fact that the absolute irreducibility of ϕ implies the non exceptional APN property, we can summarize the above discussion in the following theorem.

Theorem 5.1. For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$ where $\deg(h) = 2^s + 1 < 2^k + 1$. Then:

a) If $(k, s) = 1$, then f is not exceptional APN.

b) If $(k, s) \neq 1$ and h contains a term of degree m such that $(\phi_{2^k+1}, \phi_m) = 1$, then f is not exceptional APN.

In this theorem, the condition of the part b is best possible in the sense that if h does not have such a term, then $\phi(x, y, z)$ would be reducible.

Some cases that this theorem covers, and no one theorem enumerated in section 3 do it, are the Gold degree polynomials:

$f(x) = x^{17} + h(x)$, where $\deg(h) = 9$,

$f(x) = x^{33} + h(x)$, where $\deg(h) = 5$, 9 or 17,

$f(x) = x^{65} + h(x)$, where $\deg(h) = 33$.

6 The used methods and a proposed new method

In theorem 2, Hernando and McGuire showed that for an odd degree monomial f (not a Gold or a Kasami-Welch function), the surface ϕ (related to f) has always an absolutely irreducible factor over $\mathbb{F}_2$. They got this result by the way of contradiction, using a general form of the classical Bezout's theorem for projective curves. For this proof, a computation of all the singular points of ϕ and the computation of the intersection multiplicity at these points was required. These computations becomes very difficult for non monomial functions.

In theorem 3, Aubry, McGuire and Rodier showed that for polynomials of odd degree (not a Gold and Kasami-Welch number), the projective surface $\overline{X}$ defined by ϕ have an absolutely irreducible component defined over $\mathbb{F}_2$. They proved this indirectly, by showing that the intersection $\overline{X} \cap H$ has an absolutely irreducible component, where H is the projective hyperplane at infinity. For a family of Gold degree polynomials, theorems 4 and 5, the authors proved, by contradiction, that ϕ is absolutely irreducible.

Delgado and Janwa, in theorems 6, 7 and 9, extended the results for Gold degree polynomials. They proved the absolute irreducibility of ϕ by reductions of variables, using the hyperplane section $y+z = 0$. The authors also used affine transformations to get the relatively primeness propertiy for pairs of functions ϕ_j.

For the Kasami-Welch degree case, theorem 10, Ferard, Oyono and Rodier made an adaptation of the Gold degree results in theorems 4 and 5.

On the other hand, for even degree families ($\deg(f) = 2e$), the authors of theorem 12 applied similar arguments of theorem 3. Finally, Caullery in theorem 14 ($\deg(f) = 4e$) generalized the result of Rodier in theorem 13. The author proved that, assuming that the function f is exceptional APN, f have a very particular form. Then, he showed that f is CCZ-equivalent to a non exceptional APN function, leading to a contradiction.

As commented at the beginning of this section, a complete analysis of singular points and intersection multiplicities for polynomials with more than 2 terms is a very hard task. Max Noether's theorem, under certain conditions, could provide a new way to prove the absolute irreducibility of ϕ.

Let $p \in \mathbb{P}^2(L)$, F and G projective curves with no common components through p. Noether's conditions are satisfied at p with respect to F, G and H if there exist $a, b \in O_p(\mathbb{P}^2)$ such that $H_* = aF_* + bG_*$, where $O_p(\mathbb{P}^2)$ is the local ring of $\mathbb{P}^2$ at p and the asterisk indexes means the affine part of the curves.
If F, G and H are projective plane curves in $\mathbb{P}^2(L)$ such that F and G have no common components, then Max Noether's Fundamental theorem [11] says that exist forms A, B such that $H = AF + BG$ if and only if Noether's conditions are satisfied for every $p \in F \cap G$.

When assuming that the surface $\phi(x, y, z)$, related to a polynomial function f, is not absolutely irreducible and factors as in (4), the following pair of equations result

$$P_s Q_t = \phi_n \tag{5}$$

$$P_s Q_{t-e} + P_{s-e} Q_t = \phi_d \tag{6}$$

where P_i, Q_i are zero or forms of degree i in the variables x, y, z.

For $n = 2^k + 1$ or $n = 2^{2k} - 2^k + 1$, the forms P_s, Q_t have no common components because of the factorization of $\phi_n(x, y, z)$ [14]. If we know that Noether's conditions, with respect to P_s, Q_t and ϕ_d, are not satisfied for some $p \in P_s \cap Q_t$, then equation (6) is not possible and ϕ is absolutely irreducible, implying that f is not exceptional APN.

As an application of this method, let the Gold degree polynomial $f(x) = x^9 + h(x)$, where $\deg(h) = 7$, and $\phi(x, y, z)$ its related surface. Let $p = (1, 1, 1)$. $p \in P_s \cap Q_t$ and P_s, Q_t have no common components through p because of the factorization of $\phi_n(x, y, z)$ as product of different linear factors. Let us show that Noether's conditions, with respect to P_s, Q_t and ϕ_9, are not satisfied at p. Suppose by a contrary fact that the conditions are satisfied. Then there exist $a, b \in O_p(\mathbb{P}^2)$ such that

$$a(P_s)_* + b(Q_t)_* = (\phi_7)_*$$

where $(P_s)_*(Q_t)_* = \prod(x + \alpha y + 1 + \alpha)$, $\alpha \in \mathbb{F}_8$, $\alpha \neq 0, 1$ [14]. Then, for $y = 1$:

$$a(x, 1, 1)(x + 1)^i + b(x, 1, 1)(x + 1)^j = x^4 + x^2 + 1$$

where $i + j = 6$, $i \geq 1, j \geq 1$. But this is not possible since, in this last equation, $(x + 1)$ divides the left hand side but does not divides the right hand side. Therefore Noether's conditions are not satisfied at p and f is not exceptional APN.

As a second application, let the Kasami-Welch degree polynomial $f(x) = x^{13} + h(x)$, $\deg(h) = 7$, $\phi(x, y, z)$ its related surface and $p = (1, 1, 1)$. As before, $p \in P_s \cap Q_t$ and P_s, Q_t have no common components through p [14]. Let us suppose that Noether's conditions, with respect to P_s, Q_t and ϕ_{13}, are satisfied at p. Then

$$a(P_s)_* + b(Q_t)_* = (\phi_7)_*$$

for some $a, b \in O_p(\mathbb{P}^2)$.

In [14], a factorization of $\phi_{13}(x, y, 1)$ is provided. Using this fact, and making $y = 1$ we get:

$$a(x, 1, 1)(x^5+x^4+x^3+x^2+x+1)+b(x, 1, 1)(x^5+x^4+x^3+x^2+x+1) = x^4+x^2+1$$

Which is not possible by the same reason in the first application, and f is not exceptional APN.

Remark 1. The following remarks can clarify a little bit more about the applications of the proposed method.

(a) In the first application, the absolute irreducibility of f is already guaranteed by Delgado and Janwa in theorem 6 of section 3. However, this is not the case for the Kasami-Welch application. Theorem 9 of section 3 requires an additional absolutely irreducible condition for ensuring the irreducibility of f. Similar applications can be do it for higher Gold and Kasami-Welch degree polynomials.

(a) Both previous applications use explicit factorization of the Gold and Kasami-Welch monomial functions in order to guarantee the impossibility of the Noether's conditions. Many times this is not an easy task. Then, the usefulness of this new method depends on finding criteria for Noether's conditions to not apply at some particular point.

References

[1] I. Aubry, G. McGuire, F. Rodier: *A Few More Functions That Are Not APN Infinitely Often*, Finite Fields: Theory and Applications. Contemporary Mathematics. **518** (2010), 23-31.

[2] T.P. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy: *On Almost Perfect Nonlinear Functions Over F_{2^n}*, IEEE Transactions on Information Theory. **52** (2006), 4160-4170.

[3] E. Biham, A. Shamir: *Differential cryptanalysis of DES-like cryptosystems*, Finite Fields: Theory and Applications. Contemporary Mathematics. **4** (1991), 3-72.

[4] A. Canteaut: *Differential cryptanalysis of Feistel ciphers and differentially uniform mappings*, Selected Areas on Cryptography, SAC97. (1997), 172-184.

[5] C. Carlet, P. Charpin, V. Zinoviev: *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Designs, Codes and Cryptography. **15** (1998), 125-156.

[6] F. Caullery, *A new large class of functions not APN infinitely often*, Designs, codes and cryptography. **73** (2014), 601-614.

[7] M. Delgado, H. Janwa, *On The Conjecture on APN Functions*, arXiv:1207.5528v1[cs.IT]. (2012).

[8] M. Delgado, H. Janwa, *Progress Towards the Conjecture on APN Functions and Absolutely Irreducible Polynomials*, arXiv:1602.02576 [math.NT]. (2016).

[9] M. Delgado, H. Janwa, *On the conjecture on APN functions and absolute irreducibility of polynomials*, Designs, Codes and Cryptography. (2016), 1-11.

[10] E. Férard, *On the irreducibility of the hyperplane sections of Fermat varieties in P^3 in characteristic 2*, Advances in Mathematics of Communications. **8** (2014), 497-509.

[11] W. Fulton, *Algebraic Curves*, Universit de Versailles. (2005).

[12] S. Ghorpade, G. Lachaud, *Etale cohomology, Lefschetz theorem and number of points of singular varieties over finite fields*, Mosc. Math. J. **2** (2002), 589-631.

[13] F. Hernando, G. McGuire, *Proof of a Conjecture on the Sequence of Exceptional Numbers, classifying cyclic codes and APN functions*, Journal of algebra. **343** (2011), 78-92.

[14] H. Janwa, M. Wilson, *Hyperplane Sections of Fermat Varieties in P^3 in Char. 2 and Some Applications to Cyclic Codes*, In International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. (1993), 180-194.

[15] H. Janwa, G. McGuire, M. Wilson, *Double Error-correcting Cyclic Codes and Absolutely Irreducible Polynomials over $GF(2)$*, Journal of Algebra. **178** (1995), 665-676.

[16] D. Jedlicka, *APN monomials over $GF(2^n)$ for infinitely many n*, Finite Fields and their Applications. **13** (2007), 1006-1028.

[17] K. Nyberg, L. R. Knudsen, *Provable security against differential attacks*, Journal of Cryptology. **8** (1995), 27-37.

[18] K. Nyberg, *Differentially uniform mappings for Cryptography*, In Workshop on the Theory and Application of of Cryptographic Techniques. (1993), 55-64.

[19] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, Contemporary Mathematics. **487** (2009), 169-181.

[20] E. Férard, R. Oyono, F. Rodier, *Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents*, Arithmetic, Geometry, Cryptography and Coding Theory. Contemporary Mathematics. **574** (2012), 27-36.

[21] F. Rodier, *Functions of degree 4e that are not APN infinitely often*, Cryptography and Communications. **3** (2011), 227-240.

[22] Shafarevich, I, *Basic algebraic geometry. 1, second edn.*, Springer-Verlag, Berlin (1994).